cuccibu

Reduce Risk, Create Value

Security awareness & compliance programma's

Samen bouwen aan een sterke veiligheidscultuur

Cuccibu x Awareways

Samen bouwen we aan een veilige digitale toekomst

Met onze partner Awareways helpen wij organisaties om hun security-, privacy- en AI awareness te versterken. De focus ligt hierbij op het realiseren van meetbare gedragsverandering en het creëren van duurzame impact.

Samen bieden wij innovatieve oplossingen om organisaties te ondersteunen in de uitdagingen van de digitale transitie. Van compliance tot risicobeheer.

We werken nationaal en internationaal voor grote en kleine organisaties in diverse sectoren, waaronder:

Financiële instellingen

Overheid

Zorg

Onderwijs

cuccibu
Reduce Risk, Create Value

X

AWAREWAYS

E-learnings | Cultuurscan | Communicatiepack | Wall of vote

Mystery guest | Datalek dropping | Conversation starters

Phishing | Smishing | Vishing | Quishing | Arcadekast

Awareness trainingen | Boardroom sessies | Escape room

Deepfake awareness experience

Altijd een passende oplossing

Programma's op maat

Shift /

Phishing simulaties

- ✓ 4 rondes
- ✓ Keuze uit 12 templates

Communicatie tips & tricks

Zelfservice ondersteuning

> 25 medewerkers

Shift Add-ons

- Wave leerplatform Light
- 6 onboarding microlearnings
- 1 doelgroep
- 1 taal
- Real-time rapportage API (PowerBI)

Ideaal voor een snelle start.
Leg een solide basis voor compliance en risico-beperking met:

- Essentiële trainingen
- Phishingsimulaties
- Standaard communicatiemiddelen

** Programma ook uit te breiden met losse interventies*

Altijd een passende oplossing

Programma's op maat

Plus

Inclusief Shift

Wave leerplatform

- 8 geconfigureerde microlearnings
- Tot 2 doelgroepen
- Nederlands of Engels
- Activiteiten Dashboard
- Real-time rapportage API (PowerBI)
- Wave thema-selector

Vrije keuze uit 85+ microlearnings
Keuze uit verschillende phishing templates
Communication pack materialen
SSO connectie (SAML)

Persoonlijke ondersteuning
> 150 medewerkers

Plus Add-ons

- Eigen (custom) Wave thema
- Sector Wave leeradvies
- Cultuurscan
- Communicatie campagne
- AI-geletterdheid contentpakket
- LTI 1.3 LMS integratie
- Extra talen

Ideaal voor meer diepgang.
Verhoog het bewustzijn met:

- Oplossingen naar keuze
- Gesegmenteerde doelgroepen
- Dynamische meertalige leerervaring

** Programma ook uit te breiden met losse interventies*

Het Wave platform

Waar leren leidt tot een verandering in gedrag

Continu leren

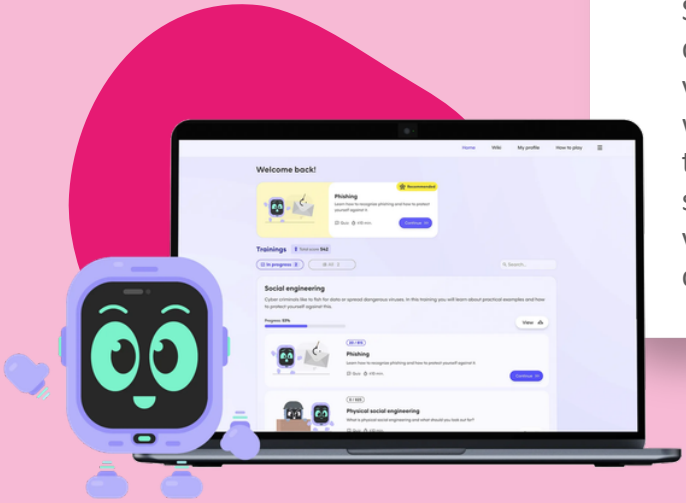
Wave is een innovatief SaaS-leerplatform dat gericht is op blijvende gedragsverandering.

Door inzichten uit psychologie, didactiek en gamification te combineren ontstaat een digitale leeromgeving die motiveert, activeert en aansluit bij de dagelijkse praktijk.

Niet alleen leren wat moet, maar toepassen wat werkt.

De kenmerken

- **Gepersonaliseerd leren.** Modules afgestemd op specifieke rollen, risico's & verantwoordelijkheden.
- **Altijd actuele content.** Toegang tot een groeiende bibliotheek met 85+ microlearnings over o.a. informatiebeveiliging, privacy, integriteit, NIS2 en AI-geletterdheid.
- **Interactief en praktijkgericht.** Scenario-gebaseerde quizzen, sectorspecifieke video's en skillgames waarin deelnemers kennis toepassen in realistische situaties, opgebouwd volgens de Miller competentiepiramide.

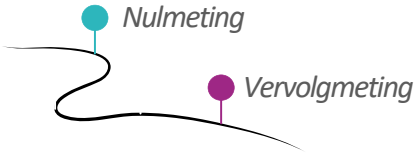


De cultuurscan

Inzicht dat beweging creëert

Jaarlijks meetbaar

Met onze cultuurscan brengen we jaarlijks de ontwikkeling van jullie informatiebeveiligings-cultuur in kaart. Data en gedragsinzichten vormen daarbij het fundament.



We starten met een nulmeting om de huidige situatie scherp te krijgen. Na 12 maanden voeren we een vervolgmeting uit.

Zo zien we niet alleen waar jullie staan, maar vooral welke vooruitgang er is geboekt in volwassenheid en gedrag.

Wat levert het op?

- **Een eerlijk beeld.** Een duidelijk en objectief beeld van de huidige volwassenheid van de organisatie.
- **Datagedreven inzicht.** Datagedreven inzicht als basis voor gerichte en effectieve interventies.
- **Aantoonbaar resultaat.** Aantoonbare verbetering in weerbaarheid en veilig gedrag.
- **Concrete handvatten.** Concrete handvatten voor het management om de informatiebeveiligings-cultuur structureel te versterken.

Van nulmeting naar aantoonbare groei in securitybewustzijn.

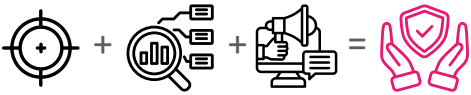
Het communicatiepack

Van bewustwording naar blijvend gedrag

Impactvolle communicatie

Gedragsverandering vraagt om consistente en relevante communicatie. Medewerkers moeten begrijpen waarom informatie-veiligheid belangrijk is en zich gesteund voelen om dagelijks veilig te handen.

Wij ontwikkelen een doorlopende communicatiestrategie op basis van de inzichten uit jullie cultuurscan én passend bij de organisatie.



Zo realiseren we gerichte, datagedreven campagnes die aantoonbaar bijdragen aan blijvende gedragsverandering.

Wat levert het op?

- **Een sterk verhaal.** Een krachtige en eenduidige verhaallijn, volledig geïntegreerd in jullie programma.
- **Een goede mix.** Een mix van communicatiemiddelen (zoals narrowcasting, video's en e-mails) rond actuele en relevante thema's.
- **Structurele aandacht.** Structurele aandacht voor het verankeren van veilig gedrag in de dagelijkse organisatiecultuur.

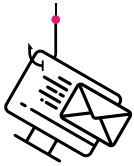
Strategische communicatie die veiligheid zichtbaar, begrijpelijk en toepasbaar maakt.

Social engineering simulaties

Oefenen met realistische dreigingen om veilig gedrag te versterken.

Interactieve simulaties

Phishing, smishing, vishing en quishing zijn dagelijkse risico's.



Met interactieve simulaties leren medewerkers deze aanvallen herkennen en juist te reageren.

Onze aanpak, gebaseerd op gedrags-wetenschap, richt zich op leren en positieve gedragsverandering in plaats van het bestraffen van fouten. Zo versterken we de menselijke verdedegingslinie.


Phishing


smishing


vishing


quishing

Phishing-simulaties kunnen het klikgedrag op kwaadaardige berichten met meer dan 90% verlagen en een ROI tot 500% realiseren.

Bron: Oosterman Research

Wat levert het op?

- **Meer bewustzijn.** Groter bewustzijn en betere herkenning van social engineering technieken.
- **Minder kans op incidenten.** Minder risico op beveiligingsincidenten.
- **Betere gewoontes.** Sterkere cyberveilige gewoonten, zoals het actief melden van verdachte berichten.
- **Realtime inzichten.** Realtime inzichten via duidelijke data en rapportages.

Adaptieve strategieën

Gepersonaliseerde leerpaden voor iedere medewerker. Wie vaker klikt, ontvangt gerichte vervolgsimulaties en aanvullende training. Alert gedrag wordt juist positief bekrachtigd.

Multichannel aanpak

Inzet via één kanaal of een gecombineerde strategie, afgestemd op jullie risicoprofiel. Van e-mail en sms tot Whatsapp, telefonische aanvallen en QR-codes.

Een mystery guest bezoek

Leren wat werkt in de dagelijkse praktijk

Praktijkgericht leren

Hoe goed ondersteunen de inrichting, werkwijzen en procedures veilig gedrag in het dagelijkse werk?

Met een mystery guest (fysieke pentest) brengen we dit op een laagdrempelige en leergerichte manier in kaart.

Door realistische situaties te observeren ontdekken we in de praktijk waar processen goed helpen, en waar ze beter kunnen.

De uitbreidingen

USB drops

Twee varianten op de werkvloer:

- USB met automatische trigger om te toetsen of maatregelen goed werken.
- USB met informatieve flyer om bewustzijn over usb-risico's te vergroten.

Datalek dropping

Fictieve persoonsgegevens worden achtergelaten om te zien of meldprocessen duidelijk en werkbaar zijn.

Wat levert het op?

- **Inzicht in de uitvoering.** Inzicht in hoe procedures en maatregelen in de praktijk worden toegepast.
- **Concrete verbeterpunten.** Concrete aanknopingspunten om processen, instructies en tooling te verbeteren.
- **Meer bewustwording.** Bewustwording door herkenbare, real-life situaties.
- **Basis voor verbeteracties.** Sterke basis voor gerichte verbeteracties binnen het awareness programma.

Wall of Vote

Laat je stem zien, live op locatie!

Live discussies

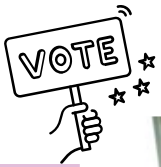
De Wall of Vote brengt een week lang interactie en discussie op de werkvloer.

Medewerkers kunnen hun mening geven over actuele en uitdagende dilemma's rondom informatieveiligheid.

Zo stimuleren we een levendige cultuur van bewustzijn en betrokkenheid. Door de Wall of Vote gebeurd dit op een interactieve, energieke manier die de dialoog over informatiebeveiliging écht op gang brengt.

Waarom?

- Fysieke interventie, wat een mooie afwisseling is met alle digitale acties.
- Brengt informatie-beveiliging tot leven.
- Een échte gespreksstarter.
- Medewerkers kunnen hun eigen mening geven, maar zien ook de reacties van collega's (sociale norm).



Conversation starters

Uitdagende dilemma's die het gesprek starten

Ga de discussie aan

Ga het gesprek aan over lastige dilemma's rondom informatiebeveiliging met onze Conversation Starter Game.

Collega's worden geconfronteerd met uitdagende en realistische scenario's die hun kritisch denkvermogen en besluitvaardigheid op de proef stellen.

Zo leren ze niet alleen de juiste keuze te maken om de organisatie te beschermen, maar ontstaat er ook een levendig gesprek over informatiebeveiliging dat bewustzijn en betrokkenheid vergroot.

Waarom?

- **Aanpasbaar.** Op maat voor maximale impact.
- **Divers.** Meerdere spelvormen mogelijk.
- **Voor iedereen.** Geschikt voor onboarders, office & non-office.

Arcadekast

Serious gaming met een retro twist

Een eigen gamehal
Een eigen gamehal op kantoor, die serieuze vaardigheden traint?

Combineer nostalgie met educatie. Reis terug in de tijd terwijl je de moderne wereld van cyberveiligheid verkent. Speel meeslepende, leerzame games en probeer de hoogste score te behalen.

De skillgames zijn niet alleen leuk en uitdagend, ze helpen medewerkers ook belangrijke cybersecurity vaardigheden te ontwikkelen.

Waarom?

- Train gedragsvaardigheden met 3 games.
- Creëer een échte eyecather in de ruimte.
- Verhoog deelname aan het security awareness programma.
- Creëer een competitie met het leaderboard.

Een gegarandeerde eyecatcher en een speelse , impactvolle aanvulling op elk security awareness programma

Onze arcadekasten zijn volledig aan te passen aan jullie huisstijl, of kies voor één van onze standaard blikvangers.

Cybersecurity escape room

Ontsnap aan cyberdreigingen!

Vind een weg naar buiten

Stap in een wereld vol spannende uitdagingen met onze unieke escape room ervaring. Werk samen als team onder tijdsdruk om puzzels op te lossen, codes te kraken en mysteries te ontrafelen.

Tijdens het spel leren deelnemers belangrijke lessen over informatieveiligheid, alertheid en effectieve samenwerking.

Een onvergetelijke ervaring die blijft hangen én medewerkers actief betrekt bij cybersecurity.

Zowel fysiek als digitaal beschikbaar.

Wanneer inzetten?

- **Teambooster**. Geschikt voor office & non-office teams.
- **Onboarding.** Ideale manier om nieuwe collega's te introduceren in het programma.
- **Cybersecurity maand.** Perfect in te zetten bij evenementen of grotere acties.

Boardroom sessies

Grip en inzicht op cyber- en digitale risico's voor bestuurders

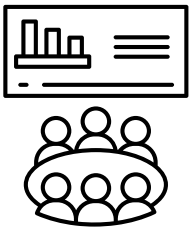
Strategisch risicobewustzijn
Onze boardroom sessies zijn korte, interactieve trainingsmomenten van 2 tot 3 uur. Speciaal ontworpen voor bestuurders.

Praktische voorbeelden, casestudies en interactieve discussies helpen bestuurders complexe onderwerpen te vertalen naar concrete strategieën en besluiten.

Zo versterken deze sessies risicobewustzijn, governance, strategische sturing én bieden ze handvatten om processen en besluitvorming structureel te verbeteren.

In één oogopslag

- Cyberrisico's in beeld.
- Risicobewust bestuur.
- Slimme besluitvorming.
- Boardroom interactie.
- Governance vertaald.
- Concrete strategieën.
- Regels eenvoudig gemaakt.
- Continuïteit en veerkracht versterken.



Tijdens deze sessies krijgt het bestuur inzicht in:

- Cyber- en digitale risico's.
- De impact van relevante wet- en regelgeving.
- De bestuurlijke verantwoordelijkheid voor veilige en continuïteitsbestendige organisaties.

**Inclusief certificaat als bewijs van deelname*

Medewerkers sessies

Veilig en bewust handelen in de dagelijkse praktijk

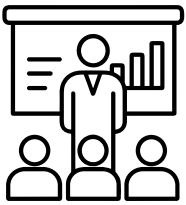
Bewustwording voor iedereen
Onze awareness sessies zijn korte, interactieve trainingsmomenten van 1 tot 2 uur. Speciaal ontworpen voor medewerkers.

Praktische voorbeelden, casestudies en interactieve opdrachten maken complexe onderwerpen begrijpelijk en direct toepasbaar. Zo versterken deze sessies bewustzijn, veilig gedrag en digitale weerbaarheid.

Elke sessie wordt vooraf afgestemd op de specifieke behoeften van de organisatie, waardoor de inhoud relevant en gepersonaliseerd is.

In één oogopslag

- Privacy & AVG.
- Informatiebeveiliging.
- NIS2 / Cbw.
- Cyber security risico's.
- Veilig gedrag in systemen.
- Digitale weerbaarheid.
- Risicoherkenning en preventie.
- Praktische tools en handvatten.



Tijdens deze sessies krijgen medewerkers:

- Inzicht in privacy, informatiebeveiliging en cyberrisico's.
- Leren zij hoe hun dagelijkse gedrag bijdraagt aan een veilige en weerbare organisatie.

Deepfake awareness experience

Inzicht in digitale risico's met AI

Herken jij AI deepfakes?
Onze 'deepfake awareness experience' zorgt ervoor dat op een innovatieve manier medewerkers bewust worden gemaakt van digitale risico's en manipulatie die mogelijk is met AI.

Met behulp van AI creëren we een realistisch deepfake filmpje van een medewerker, directeur of manager, waarin een vooraf besproken boodschap wordt overgebracht. Het filmpje wordt binnen de organisatie getoond en illustreert op een tastbare manier hoe overtuigend en toegankelijk dit soort technologie inmiddels is.

Over de video

- Positieve en verantwoorde benadering.
- Boodschap stemmen we af met de organisatie.
- Elke video sluit af met een duidelijke waarschuwing dat het AI gegeneerd is.

Zo ervaren medewerkers de gevaren van deepfakes, leren ze kritisch kijken naar digitale content en versterken ze hun bewustzijn en digitale weerbaarheid.

cuccibu

Reduce Risk, Create Value

Maak van medewerkers je sterkste schakel

Informatiebeveiliging en privacy gaan verder dan techniek alleen. Echte digitale weerbaarheid ontstaat wanneer medewerkers risico's herkennen, veilige keuzes maken en bewust omgaan met informatie. Structurele awareness helpt organisaties om incidenten te voorkomen, compliance te versterken en een sterke securitycultuur op te bouwen.

Even sparren over de mogelijkheden van onze **Security Awareness & Compliance programma's** voor jouw organisatie?

Neem vrijblijvend contact met ons op.

sales@cuccibu.nl +31 (0)85 303 2984

Of neem een kijkje op de website.

https://cuccibu.com/information-security/security-en-privacy-awareness/